Smart Grid Interoperability Panel (SGIP)
Cyber Security Working Group (CSWG)
Standards Review

CSWG Standards Review Report

ANSI C12.22-2008

May 10, 2011

Security Assessment of ANSI C12.22-2008

1. Introduction

1.1 Correlation of Cybersecurity with Information Exchange Standards

Correlating cybersecurity with specific information exchange standards, including functional requirements standards, object modeling standards, and communication standards, is very complex. There is rarely a one-to-one correlation, with more often a one-to-many or many-to-one correspondence.

First, communication standards for the Smart Grid are designed to meet many different requirements at many different "layers" in the communications "stack" or "profile," one example of such a profile is the GridWise Architecture Council (GWAC) Stack. Some standards address the lower layers of the communications stack, such as wireless media, fiber optic cables, and power line carrier. Others address the "transport" layers for getting messages from one location to another. Still others cover the "application" layers, the semantic structures of the information as it is transmitted between software applications. In addition, there are communication standards that are strictly abstract models of information – the relationships of pieces of information with each other. Since they are abstract, cybersecurity technologies cannot be linked to them until they are translated into "bits and bytes" by mapping them to one of the semantic structures. Above the communications standards are other security standards that address business processes and the policies of the organization and regulatory authorities.

Secondly, regardless of what communications standards are used, cybersecurity must address all layers – end-to-end – from the source of the data to the ultimate destination of the data. In addition, cybersecurity must address those aspects outside of the communications system in the upper GWAC Stack layers that may just be functional requirements or may rely on procedures rather than technologies, such as authenticating the users and software applications, and screening personnel. Cybersecurity must also address how to: cope during an attack, recover from it afterwards, and create a trail of forensic information to be used in post-attack analysis.

Thirdly, the cybersecurity requirements must reflect the environment where a standard is implemented rather than the standard itself: how and where a standard is used must establish the levels and types of cybersecurity needed. Communications standards do not address the importance of specific data or how it might be used in systems; these standards only address how to exchange the data. Standards related to the upper layers of the GWAC Stack may address issues of data importance.

Fourthly, some standards do not mandate their provisions using "shall" statements, but rather use statements such as "should," "may," or "could." Some standards also define their provisions as being "normative" or "informative." Normative provisions often are expressed with "shall" statements. Various standards organizations use different terms (e.g., standard, guideline) to characterize their standards according to the kinds of statements used. If standards include security provisions, they need to be understood in the context of the "shall," "should," "may," and/or "could" statements, "normative," or "informative" language with which they are expressed.

Therefore, cybersecurity must be viewed as a stack or "profile" of different security technologies and procedures, woven together to meet the security requirements of a particular implementation of a stack of policy, procedural, and communication standards designed to provide specific services. Ultimately, cybersecurity as applied to the information exchange standards should be described as profiles of technologies and procedures which can include both "power system" methods (e.g. redundant equipment, analysis of power system data, and validation of power system states) and information technology (IT) methods (e.g. encryption, role-based access control, and intrusion detection).

There also can be a relationship between certain communication standards and correlated cybersecurity technologies. For instance, if TCP/IP is being used at the transport layer and if authentication, data integrity, and/or confidentiality are important, then TLS (transport layer security) should most likely (but not absolutely) be used.

In the following discussions of information exchange standard(s) being reviewed, these caveats should be taken into account.

1.2 Correlation of Cybersecurity Requirements with Physical Security Requirements

Correlating cybersecurity requirements with specific physical security requirements is very complex since they generally address very different aspects of a system. Although both cyber and physical security requirements seek to prevent or deter deliberate or inadvertent attackers from accessing a protected facility, resource, or information, physical security solutions and procedures are vastly different from cybersecurity solutions and procedures, and involve very different expertise. Each may, in fact, be used to help protect the other, while compromises of one can definitely compromise the other.

However, physical and environmental security that encompasses protection of physical assets from damage is addressed by the NISTIR 7628 only at a high level. Therefore, assessments of standards that cover these non-cyber issues must necessarily also be at a general level.

1.3 Standardization Cycles of Information Exchange Standards

Information exchange standards, regardless of the standards organization, are developed over a time period of many months by experts who are trying to meet a specific need. In most cases, these experts are expected to revisit standards every five years in order to determine if updates are needed. In particular, since cybersecurity requirements were often not included in standards in the past, existing communication standards often have no references to security except in generalities, using language such as “appropriate security technologies and procedures should be implemented.”

With the advent of the Smart Grid, cybersecurity has become increasingly important within the utility sector. However, since the development cycles of communication standards and cybersecurity standards are usually independent of each other, appropriate normative references between these two types of standards are often missing. Over time, these missing normative references can be added, as appropriate.

Since technologies (including cybersecurity technologies) are rapidly changing to meet increasing new and more powerful threats, some cybersecurity standards can be out-of-date by the time they are released. This means that some requirements in a security standard may be inadequate (due to new technology developments), while references to other security standards may be obsolete. This rapid improving of technologies and obsolescence of older technologies is impossible to avoid, but may be ameliorated by indicating minimum requirements and urging fuller compliance to new technologies as these are proven.

1.4 References and Terminology

References to the National Institute of Standards and Technology (NIST) security requirements refer to the NIST Interagency Report (IR) 7628, *Guidelines to Smart Grid Cyber Security*, Chapter 3, High-Level Security Requirements.

References to “government-approved cryptography” refer to the list of approved cryptography suites identified in Chapter 4, Cryptography and Key Management, of NISTIR 7628. Summary tables of the approved cryptography suites are provided in Chapter 4.3.2.1.

As noted, standards have different degrees for expressing requirements, and the security requirements must match these degrees. For these standards assessments, the following terminology is used to express these different degrees[1]:

- Requirements are expressed by "…shall…," which indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).
- Recommendations are expressed by "…should…," which indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).
- Permitted or allowed items are expressed by "…may…," which is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).
- Ability to carry out an action is expressed by "…can …," which is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).
- The use of the word *must* is deprecated, and should not be used in these standards to define mandatory requirements. The word *must* is only used to describe unavoidable situations (e.g. "All traffic in this lane must turn right at the next intersection.")

2. ANSI C12.22-2008

2.1 Description of Document

This standard was developed jointly by ANSI (published as ANSI C12.22-2008), IEEE (to be published as IEEE 1703-2011) and Measurement Canada (to be published as MC12.22-2011). The joint development agreement was formalized through a Memorandum of Understanding (MOU) that was signed by Measurement Canada (for the Measurement Canada Task Force for Electronic Metering Devices), NEMA (for ANSI C12 SC17) and IEEE (for IEEE SCC31). The purpose of the MOU is to "To develop a standard for Protocol Specification for Interfacing to Data Communication Networks, jointly…", and "In view of the joint development of the Work, it is the belief of the organizations that opportunities exist to coordinate with each other in the independent development and publication of the Work which will provide a benefit to the end users. To accomplish this goal, IEEE, NEMA and MC agree to openly communicate with each other regarding the status of the Work." [Ref. C12.22 MOU, 2007]. As a direct consequence of the MOU, the three standards are cyclically published in a manner that maintains their mutual coherence. At the time of this review ANSI C12.22-2008 was published. IEEE P1703-2010 was successfully balloted and is in the comment resolution phase, and MC12.22 is pending publication using the approved IEEE 1703 standard as the reference document. IEEE P1703-2010 includes an extra Annex K, "Listing of Editorial Errors and Errors of Omission in ANSI C12.22-2008," that is absent in ANSI C12.22-2008. This annex contains corrections and information for consideration by ANSI C12 SC 17 WG 1, the joint work group that is responsible for the next maintenance release of ANSI C12.22.

These three versions of the Standards are commonly and generically referred to as ANSI C12.22 by the industry.

The purpose of the ANSI C12.22 standard is to define the network framework and the means to transport the Utility End Device Data Tables via any reliable network, such as a Local Area Network (LAN) or Wide Area Network (WAN) for use by metering or enterprise systems in a multi-vendor sourced environment.

[1] The first clause of each terminology definition comes from the International Electrotechnical Commission (IEC) Annex H of Part 2 of ISO/IEC Directives. The second clause (after "which") comes from the Institute of Electrical and Electronics Engineers (IEEE) as a further amplification of the term.

The ANSI C12.22 Standard accomplishes its objectives by providing a managed, adaptive and secured message delivery system for End Devices (e.g. meters) and ancillary devices (e.g. home appliances and communication infrastructure technology) that implement an “end-to-end” messaging system, i.e. connecting meters with the enterprise AMI environment and the customer (consumer) environment, in a manner that is completely independent from network transport used.

The ANSI C12.22 Standard extends the definitions provided by ANSI C12.19-2008 (IEEE P1377-2010) to include provisions for network interface tables and relay management tables and interface security tables. It also introduces services that automate the deployment, subscription and presence of C12.22 Nodes on an AMI (Advanced Metering Infrastructure) network.

The standard is sectioned as follows:

- Section 1 is an Overview that covers the scope of the standard and its purpose.
- Section 2 contains normative and informative references.
- Section 3 describes the document terminology and syntax construction rules.
- Section 4 is the reference topology. This section describes possible interactions between network assets (C12.22 Nodes). It also identifies the various ways one can bind a device to a communication module using internal and external buses.
- Section 5, C12.22 Node to C12.22 Network Segment Details, and Annex J, Connectionless-ACSE- Equivalent Reduced Syntax for C12.22 Message Transmission, describe the generic and common C12.22 Node interface to a C12.22 Network segment. It includes definitions of message element encoding rules and the C12.22 application services.
- Section 6, Protocol Details: C12.22 Device to C12.22 Communication Module Interface, describes the interface requirements and services used to interface a C12.22 Device (e.g. the metrology component of a meter) to a C12.22 Communication Module (e.g. a network adapter).
- Section 7, Local Port Communication Protocol Details, describes the protocol and interface requirements for internal generic and dedicated interfaces to network and peripherals (e.g. MODEM). It also describes the detailed implementation of a local ANSI Type 2 optical port communication. This C12.22 ANSI Type 2 protocol is backward compatible with ANSI C12.18-2008 protocol.
- Section 8 describes the compliance assumptions of ANSI C12.22, ANSI C12.21 and ANSI C12.18.
- Annex A, Relays, Annex B, Routing examples, Annex D, Universal Identifier and Annex F, APDU Response Timeout Algorithm, describe the implementation model of ANSI C12.22 Relays and Relays. It also covers C12.22 Node naming and the management techniques necessary to maintain an operational C12.22 Network.
- Annex C, contains extensions to ANSI C12.19-2008 in the form of C12.19 Tables and procedures necessary to manage a C12.22 Network and its C12.22 Nodes.
- Annex E, One Way Devices, describe a special case of a simplified C12.22 Message for use by legacy simple one-way communicating devices.
- Annex G, Communication Examples and Annex H, CRC Examples provide examples for developers.
- Annex I, The EAX’ Encryption Mode, describes the implementation of the EAX’ cryptographic model and provides justification for its use. The justification is needed to explain the selection of EAX’ in lieu of CCM and optimizations of EAX’ from EAX.

ANSI C12.22 accommodates interconnections among C12.22 Nodes that may be located on the same network or on different networks. ANSI C12.22 Messages are forwarded across different networks using ANSI C12.22 Relays. ANSI C12.22 Relays and ANSI C12.22 Master Relays are managed; where ANSI C12.22 Master Relays provide node-name subscription and resolution services. ANSI C12.22 Node-names are known as "Application Titles" (or ApTitles) and are globally unique.

ANSI C12.22 uses a "reduced stack" model, where OSI layers 7, 6 and 5 are collectively used as the C12.22 Application Layer. ANSI C12.22 defines the following OSI protocol stacks:

1. Application layer interface to unspecified ISO Layers 4, 3, 2 and 1. This provides only application layer definitions for services and application layer payloads that can be communicated over any transport, network, data link and physical layer.
2. Providing a full stack definition for interfacing a C12.22 Device to an external C12.22 Communication Module. This was accomplished by defining the physical interface requirements between the C12.22 Device (e.g. a meter) and the C12.22 Communication Module (e.g. a network transceiver), and defining the interface lower layers: 4 (transport), 3 (network), 2 (data link) and 1 (physical). The C12.22 Communication Module is not trusted by the C12.22 Device, therefore the C12.22 Device is in full control of the communication module and of the C12.22 Message Security.
3. Providing a full stack definition for point-to-point communication to be used over ANSI Type 2 local ports. This was accomplished by defining a Layer 4 (transport) and Layer 2 (data link) and Layer 1 (physical). The ANSI Type 2 optical port protocol is backward compatible with ANSI C12.18-2008, however it has been extended to support the full ANSI C12.22 secured and reliable network communication.
4. Providing support for efficient one-way messaging (blurts).This is an alternate Application layer interface message that defines a compact message format that can be easily transformed into a standard ANSI C12.22 Datagram, and assuming that all needed layers defined in this Standard can support one-way messaging. The ANSI C12.22 Blurt support network is not defined by the standard. Therefore it is required that the implementer of the one-way blurt-network provide a C12.22 Gateway into the proper ANSI C12.22 Network Segment. The C12.22 Gateway is the "trusted agent" in this case.

ANSI C12.22 defines the assets that may be found on a C12.22 Network. Any ANSI C12.22 Network asset is a C12.22 Node and it must be registered on the network in order to be able to communicate on the network. ANSI C12.22 Nodes are classified as follows:

1. C12.19 Device, a C12.22 Node that contains ANSI C12.19 and ANSI C12.22 Tables.
2. C12.22 Host, a C12.22 Node that typically runs on a computer and it is not necessarily an embedded system.
3. C12.22 Authentication Host, a C12.22 Host that is an authoritative administrative agent for registering C12.22 Nodes for a given ANSI C12.22 Master Relay of a network service provider's domain. ANSI C12.22 Nodes communication privileges required authorization by an authoritative C12.22 Authentication Host that is trusted by the ANSI C12.22 Master Relay.
4. C12.22 Notification Host, a C12.22 Host, which contains an application that needs to be notified when C12.22 Nodes join or leave the C12.22 network. Examples of C12.22 Notification Hosts include billing systems, emergency response systems and in-home energy management systems, which need to communicate or control other C12.22 Nodes.
5. C12.22 Relay, a C12.22 Node that provides name (ApTitle) to native network address resolution services and C12.22 Message forwarding to other C12.22 Nodes that do not reside on the same C12.22 Network Segment. ANSI C12.22 Network Segment policy governs whether C12.22 Nodes may communicate directly with other C12.22 Nodes on the same C12.22 Network Segment

(neighboring C12.22 Nodes) or whether the nodes use a C12.22 Relay to communicate with each other.

6. C12.22 Master Relay, a C12.22 Relay that operates at the top of a hierarchy of C12.22 Relays of a network service provider's domain. It provides registration services of all C12.22 Nodes in its domain. C12.22 Master Relays communicate with C12.22 Authentication Hosts to manage network security and access privileges. C12.22 Master Relay communicates with C12.22 Notification Hosts to provide them with information about C12.22 assets that are accessible on the C12.22 Network.
7. C12.22 Gateway, a C12.22 relay that in addition has a capability to translate and bridge between ANSI C12.22 protocol and non ANSI C12.22 protocols.

2.2 Assumptions

ANSI C12.22-2008 is basically an application communication message delivery protocol that relies on other standards to provide the payload data (e.g. ANSI C12.19-2008), network application message wrapper (e.g. ISO/IEC 10035-1) and message delivery system (e.g. IETF RFC 793). ANSI C12.22 specifies minimum requirements for the implementation of the protocol and it describes a number of optional services and security modes.

2.3 Assessment of Cybersecurity Content

ANSI C12.22 assumes that an external governance policy (e.g. security requirements, such as NISTIR) will be used to establish specific minimum requirements. The security role of ANSI C12.22 ends upon delivery of a validated and optionally authenticated or decrypted message to the C12.22 Node's embedded application entity. For example, the role-based access control requirements for table data is delegated to ANSI C12.19-2008 and is expected to be enforced by the C12.19 Device firmware implementation.

ANSI C12.19-2008 provides specific guidance to implementers of table data delivery systems, such as ANSI C12.22, on compliance and operational requirements for Table (payload) read and write operations (see Section 8 of ANSI C12.19-2008). For these reasons the ANSI C12.22-2008 standard does not concern itself with any consequence of operations that follow the successful delivery of the payload data to its upper application layer or its lower transport layers of the OSI protocol stack.

2.3.1 Does the standard address cybersecurity? If not, should it?

The ANSI C12.22-2008 standard addresses those aspects of cyber security that are deemed to be within its end-to-end and any-network communication scope, while making the assumption that other governance documents and policies will drive the actual implementation choice. Similarly it assumes that the network used for delivering the C12.22 Messages can be any network that can meet the cyber security policy requirements.

The ANSI C12.22 Application layer security is defined in Section 5.3.4.13, C12.22 Security Mechanism, of the ANSI C12.22 standard. The security mechanisms include provisions for message privacy and authentication, playback rejection, and message acceptance windows as well as ANSI C12.19 role-based data access to C12.19 Devices. The ANSI C12.22 Application layer built-in (default) security mechanism provides three options to choose from when sending C12.22 Messages:

1. Sending clear text messages over the C12.22 Network. This mode of communication may result in altered C12.22 Messages and exposure to password sniffing attacks.
2. Sending authenticated plain text messages over the C12.22 Network. This mode of communication may result in password sniffing attacks.

3. Sending of authenticated cipher text over the C12.22 Network. This mode of communication provides message content, message envelope and peer C12.22 Node authentication and privacy.

When modes 1 and 2 are used, it is still possible the network or transport layers to provide for authentication and confidentiality. Otherwise, additional transport or network layer security protocols are not required by ANSI C12.22, but they can be provided (transparently to ANSI C12.22) by network integrators in order to enhance improve the security provisions cited above. However, any added transport security (e.g., TLS) or IP security (e.g., IPsec) features are expected to be an enhancement and not a substitute for the interoperable and-to-end ANSI C12.22 and ANSI C12.19 security provisions.

The ANSI C12.22 Standard allows for extension/expansion with any security mechanisms. The security mechanism extension is managed through the use object identifiers (security mechanism names) that are encapsulated inside the C12.22 Message.

However, in this standard cybersecurity is optional; this standard does not require cybersecurity to be implemented. Instead it only identifies available security features and extension mechanisms, but it leaves the final choice to the implementer. This means that implementations can be compliant with the standard while still not meeting necessary cybersecurity requirements. While perhaps accurate, this is an implementation detail that is outside the scope of the standard (i.e. the standards provides the ‘means’, but is not a ‘best practice’ for use).

The needed assumptions and requirements for a secure network implementation are deferred by the standard to governance policies and procedures are defined outside of this standard. This Standard provides only the means, not the requirements.

2.3.2 What aspects of cybersecurity does the standard address and how well (correctly) does it do so?

The correlations between this document and the security requirements described in NISTIR 7628, *Guidelines to Smart Grid Cybersecurity*, Chapter 3, families and requirements, are shown in Table 1.

Table 1: Correlations between Standard being Assessed and the NISTIR Security Requirements

Reference in Standard[2]	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
4 Reference Topology	SG.AC-6 Separation of Duties	The standard defines separation of duties and responsibilities among its assets. It identifies the different roles of C12.22 Communication Modules and C12.22 Devices (e.g. metrology portion of a meter); C12.22 Master Relays and C12.22 Authentication Hosts; C12.22 Relays and C12.22 Master Relays or C12.22 Gateway; C12.19 Devices (End Devices), C12.22 Hosts and C12.22 Notification Hosts. In addition the standard clearly specifies the operational requirements and the application context of any C12.22 Node that is implemented on a network access point.

[2] The references may be just the section numbers or could include the title of the section, depending upon what fits easily.

Reference in Standard[2]	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
4: Reference Model	SG.SC-25: Operating System Independent Applications	Because C12.22 messages can be carried over any reliable network, the system can be used with any computer operating system that properly can format C12.22 messages
5.3.4 Association Control—Association Control Service Element (ACSE)	SG.AC-4: Access Enforcement	Meets requirements if governance policy mandates it for the specific use and class of device.
5.3.2.4.2 Read Service	SG.AC-4: Access Enforcement	Access requirements are enforced by the End Device using the ANSI C12.19 role-based accessibility policy. These are not defined in this standard, instead they are managed (programmed by the service provider) in accordance with a governance policy and the specific use and class of device.
5.3.2.4.3 Write Service	SG.AC-4: Access Enforcement	Access requirements are enforced by the End Device using the ANSI C12.19 role-based accessibility policy. These are not defined in this standard, instead they are managed (programmed by the service provider) in accordance with a governance policy and the specific use and class of device.
5.3.2.3: Time Out	SG.AC-11: Concurrent Session Control	
5.3.2.3: Time Out	SG.AC-13: Remote Session Termination	
5.3.2.4.4: Logon Service	SG.AC-15: Remote Access	
5.3.2.4.5: Security Service	SG.AC-2: Remote Access Policy and Procedures SG.IA-3: Authenticator Management, SG.AC-21: Passwords	The standard allows for Passwords and User IDs to be sent in clear text. When this practice is permitted by the governance policy and implemented by the device then it may be a vulnerability. The storage of passwords in equipment is not in the scope of this standard.
5.3.2.4.6: Logoff Service	SG.AC-13: Remote Session Termination	
5.3.2.4.7: Terminate Service	SG.AC-13: Remote Session Termination	
5.3.2.4.8 Disconnect Service	SG.AC-13: Remote Session Termination	
5.3.2.4.9 Wait Service	SG.AC-15: Remote Access	
5.3.2.4.10: Registration Service	SG.AC-2: Remote Access Policy and Procedures SG.AC-3: Account Management SG.AC-6 Separation of Duties	Service information (Node type, node class, Serial number, etc.) is transferred in clear text, but may be authenticated.

Reference in Standard[2]	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
5.3.2.4.11 Deregistration Service	SG.AC-3: Account Management	It is not clear if there is authentication and authorization of the client as having appropriate privileges to perform the deregistration function. If not properly authorized, this could lead to denial of service attacks. Specifically the standard is not clear on whether the C12.22 Master Relay should prevent de-registration unless approved by a C12.22 Authentication Host.
5.3.2.4.13 Trace Service	SG.AC-3: Account Management	The Trace Service is used to retrieve the list of C12.22 Relays that are on the path between the requesting C12.22 Node and the target C12.22 Node. A C12.22 Relay may reject the request when it cannot service it for any reason, including security considerations. The response to a Trace Service request contains a list of C12.22 Relay Application Titles (names) encountered up to the point being the target C12.22 Node or the C12.22 Relay that was the point of failure (the entity that rejected the message). The Trace Message is propagated from C12.22 Relay to C12.22 Relay and it may be authenticated but not confidential. This trace information could be sensitive or spoofed – it is not clear if it requires authentication and appropriate authorization The standard does not provide explicit guidance on a best approach for mutual authentication required between the requesting C12.22 Node and the C12.22 Relay, and the forwarding C12.22 Relay to the next C12.22 Relay along the path to the C12.22 target node.
5.3.3 EPSEM Envelope Structure	SG.IA-5 Device Identification and Authentication	Bit 2 to 3: SECURITY_MODE 0 = Cleartext 1 = Cleartext with authentication 2 = Ciphertext with authentication

Reference in Standard[2]	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
5.3.4.8 Calling Authentication Value Element (ACH)	SG.AC-2: Remote Access Policy and Procedures SG.IA-5 Device Identification and Authentication	"*The optional Authentication Value Element <calling-authentication-value-element > is used to carry privacy and authentication parameters. When it contains an <calling-authentication-value-c1221> the <user-information> shall be transmitted unencrypted and the SECURITY_MODE value of the <epsem-control> field shall be set to 1*. *When <calling-authentication-value-c1222> is included then the <user-information> is authenticated and private (when the SECURITY_MODE value of the <epsem-control> field is set to 2), or just authenticated (when the SECURITY_MODE value of the <epsem-control> field is set to 1). Note that the <epsem-control> field is transmitted as Cleartext (i.e., it may be authenticated, but never encrypted)*." Transmitting user information in cleartext is a security violation.
5.3.4.8.1: C12.22 Security Mechanism	SG.IA-5 Device Identification and Authentication.	One form of message transportation is unauthenticated Clear text. When policy permits its use then it is a vulnerability.
5.3.4.8.2 C12.21 Security Mechanism	SG.IA-5 Device Identification and Authentication	In this mode passwords are sent in the clear. This is a legacy mode for tunneling C12.21 messages through C12.22 Networks.
5.3.4.8.3 C12.22 Other Security Mechanisms	SG.IA-5 Device Identification and Authentication	Just a method to use some other authentication mechanism
5.3.4.8: Calling Authentication Value Element 7: Local Port Communication Protocol Details	SG.SC-18: System Connections	
5.3.4.11: User information Element	SG.SC-12 Use of Validated Cryptography	EAX' mode is required, but it is not (yet) a NIST approved cryptographic method. EAX' is now being reviewed by NIST. The technical reason for using EAX mode is discussed in Annex I of ANSI C12.22.
5.3.4.13.1: C12.22 Security mechanism	SG.IA-5 Device Identification and Authentication	Authentication is not mandatory. When the SECURITY_MODE field is set to zero (0), all of the elements of the C12.22 Message are sent as Cleartext without any authentication and with neither <mac> nor <padding> appended at the end of the message.

Reference in Standard[2]	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
5.3.4.13.1: C12.22 Security mechanism	SG.SC-12 Use of Validated Cryptography	EAX' mode is required, but it is not (yet) a NIST approved cryptographic method. EAX' is now being reviewed by NIST. The technical reason for using EAX mode is discussed in Annex I of ANSI C12.22.
5.3.4.13.1: C12.22 Security mechanism	SG.IA-5 Device Identification and Authentication	The "built-in" default mechanism provides for three operating modes. One of the modes is not authenticated, and two of the modes are not encrypted.
5.3.4.13.1: C12.22 Security mechanism	SG.SC-11 Cryptographic Key Establishment and Management	Only pre-stored keys are referenced, thus leaving key management outside the scope of this standard.
5.3.4.13.1: C12.22 Security mechanism	SG.SC-11 Cryptographic Key Establishment and Management	EAX' mode is required, but it is not (yet) a NIST approved cryptographic method. EAX' is now being reviewed by NIST. The technical reason for using EAX mode is discussed in Annex I of ANSI C12.22.
5.3.4.13.1: Security Mechanism	SG.SC-20: Message Authenticity	
5.1 and Annex A	SG.SC-21: Secure Name/Address Resolution Service	Clause 5.1 provides for connection to a gateway to any other network. Annex A specifies address resolution requirements within C12.22 networks and supports resolutions within other networks.
Annex C.1: Table 128 Network Statistics Table	SG.AU-3: Content of Audit Records	
Annex C.1: Table 123 Exception Report Configuration Table	SG.AU-6: Audit Monitoring, Analysis, and Reporting	
Annex C1: Decade 12	SG.SI-4: System Monitoring Tools and Techniques	Table 123 can be configured to report exceptions, providing at least a component of a tool for the detection and reporting of unusual events.
4: Reference Model	SG.SI-9: Error Handling	Table 123 can be configured to report some types of errors.
C12.19 (incorporated by reference) and Clauses 4 - 7	SG.SC-9: Communication Confidentiality	Products must support the C12.19 Table protocol and the complete C12.22 protocol as specified in C12.22, Clauses 4-6. On-site protection - which helps assure message confidentiality - is provided by the Local Access specifications of Clause 7 of C12.22.
Clauses 4 - 6	SG.SC-10: Trusted Path	If all security functions are implemented, products must support the C12.19 Table protocol and the complete C12.22 protocol as specified in C12.22, Clauses 4-6. Taken together, this provides a Trusted Path option.

2.3.3 What aspects of cybersecurity does the standard not address? Which of these aspects should it address? Which should be handled by other means?

This standard has a number of concerns related to cybersecurity:

- Some cybersecurity aspects are not acceptable from a security perspective:
  - The EAX’ encryption mode is not accepted by NIST at this time. However, EAX’ will be reviewed as soon as documentation is submitted to NIST. The selection by ANSI C12.22 of EAX (rather than the NIST-approved CCM, as an example) is due to the need of C12.22 to deal with: large Nonce lengths, Nonce unpredictability, "Online" message processing capability, Authenticate-before-decrypt requirement, Block cipher independence, Hardware support of canonicalized messages.
  - It should be noted that C12.22 nonce has a long, varying length, sometimes more than 60 octets, which rules out CCM, and that many of the platforms on which it will be implemented may have hardware support for AES but will have none for modular multiplication. GCM requires a fixed length nonce, thus maximal for any instance of C12.22 use (if such can be determined reliably), and it also includes modular multiplication. EAX and EAX' thus require less computation per instance of use than GCM, better fitting the type of microcontrollers often found today in AMI metering. More details on the technical reason for using EAX mode are available in Annex I of ANSI C12.22.
  - Passwords may be sent in cleartext or plaintext, thus becoming a vulnerability, when such a practice is permitted.
- Cybersecurity that is strictly within its scope is addressed, while making the valid assumption that external policy must exist to cover the broader cybersecurity requirements.
- The standard is not well structured for understanding what cybersecurity requirements (or options) actually exist. The document mixes normative and informative items that are not clearly distinguished, and does not clearly identify the security aspects.
  - Some cybersecurity guidelines do exist in other documents, such as the AEIC document developed in PAP 5: “*SmartGrid/AEIC AMI Interoperability Standard Guidelines for ANSI C12.19 / IEEE 1377 / MC12.19 End Device Communications and Supporting Enterprise Devices, Networks and Related Accessories*”. Although focused on interoperability issues, that document did identify some cybersecurity gaps in ANSI C12.22.
  - Some other documents provide more general guidelines on implementing cybersecurity for metering systems.
- Key management is assumed to be handled elsewhere.
  - The use of security is optional.
- Some specific cybersecurity requirements and definitions are described in ANSI C12.19-2008.
  - Section 3, Definition, provides specifications for End Device, Events, Loggers, Modes, Adjustments, seals and digital signatures
  - Section 8, Table Transport Issues, provide requirements for Read and Write Services, in-bound and out of bound data reference and attempted access, use of pending tables (e.g. for deferred processing or program/firmware upload), and list index management.
  - Section 4, General, and Section 9, Tables, provide requirements for table structure and access management. For example, Table 0 is “READONLY”.
  - Annex B, History & Event Log Codes, Annex E, Event Logger Implementation, together with Section 9, Tables, provide implementation requirements for history and event (transaction) loggers.

2.3.4 What work, if any, is being done currently or is planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

- EAX' will be reviewed by NIST once documentation is submitted to NIST. The selection by ANSI C12.22 of EAX' (rather than the NIST approved CCM as an example) is due to the need of C12.22 to deal with: large Nonce lengths, Nonce unpredictability, "Online" message processing capability, Authenticate-before-decrypt requirement, Block cipher independence, Hardware support of canonicalized messages.
  - Some concern has been expressed that existing NIST-approved cryptographic suites using the GCM mode of AES, which has similar performance as EAX', have been overlooked as possible alternatives.
  - For more information in the reasons for use of EAX' see Annex I of ANSI C12.22.
- The AEIC Guidelines v2.0 was published to tighten variation.
- Event Logger requirements have been developed and are evolving (Canada)
- ANSI C12 SC17 has the mandate to begin work on ANSI C12.22 Key management protocol.
- NAEDRA (the North American End Device Registration Authority™) was formed to accredit registrars that may be used to manage the allocation and distribution of OID.
- New device data models and security algorithms can be registered through NAEDRA accredited registrars.
- MOU exists among MC/IEEE (SCC31)/ANSI (NEMA) that ensures continued synchronization of the IEEE, ANSI and MC standards and future proofing them.
- RFC 6142, "*ANSI C12.22, IEEE 1703, and MC12.22 Transport Over IP*" was created that also makes cybersecurity requirements.

More work is still needed on cyber security requirements to be placed in the standards.

2.3.5 Recommendations

The ANSI C12.22 standard contains many issues related to cybersecurity. Therefore the following recommendations are made:

- The standard should correct, through addendums or other mechanisms, the explicit issues identified in the last bullet in section 2.3.3 of this review.
- The EAX' cryptographic suite should go through the NIST review. At the same time, existing NIST-approved cryptographic suites using the GCM mode of AES should be compared for performance, vulnerabilities, and applicability to the AMI system requirements.
- One or more additional cybersecurity documents should be developed to:
  - Clarify all of the assumptions made in the C12.xx series with respect to cybersecurity.
  - Identify the exact location and implications of the cybersecurity requirements in this series of standards.
  - Provide higher level guidance for cybersecurity policies, methodologies, and technologies that are out of scope for these individual standards but that are needed for securing the networking infrastructure.

  - – Provide cybersecurity requirements for metering devices that mandate features assumed or supported by ANSI C12.22 but not mandated there. Such requirements should implement NISTIR requirements related to equipment.
- Message replay prevention, message acceptance window, and message source/destination rejection capabilities are supported by ANSI C12.22, but do not seem to be in the NISTIR.
- Only pre-stored keys are referenced in the default security mechanisms, thus leaving key management outside the scope of this standard. A new proposal was made to ANSI C12 SC17 to work on a key management add-on standard for C12.22. This is may be contributed to the SGIP for the formation of a new PAP.
- The ANSI C12.22 Standard should be revised to be more specific on whether the C12.22 Master Relay should prevent de-registration unless approved by a C12.22 Authentication Host. This way a rogue node may not cause a malicious deregistration of C12.22 Nodes from the network.

2.3.6 List any references to other standards and whether they are normative or informative.

2.3.6.1 ANSI C12.22 – Normative

ANSI C12.18-1996	Protocol Specification for ANSI Type 2 Optical Port
ANSI C12.19-1997	Utility Industry End Device Data Tables
ANSI C12.21-1999	Protocol Specification for Telephone Modem Communication
IEEE C37.90.1-2002	IEEE Standard for Surge Withstand Capability (SWC) Tests for Relays and Relay Systems Associated with Electric Power Apparatus
IEEE C62.41-2002	IEEE Recommended Practice on Surge Voltages in Low-voltage AC Power Circuits
ISO/IEC 7498-1	Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model
ISO/IEC 13239:2002	Information Technology—Telecommunications and Information Exchange between Systems—High-level Data Link Control (HDLC) Procedures—Frame Structure, Annex A, Explanatory Notes On Implementation of the Frame Checking Sequence
ANSI INCITS 92	Data Encryption Algorithm
EAX 2003	Authenticated Encryption with Associated Data (AEAD) Algorithm Designed to Simultaneously Protect both Authentication and Privacy of Messages, as Described in "A Conventional Authenticated-Encryption Mode," M. Bellare, P. Rogaway and D. Wagner, April 13, 2003, available from http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/eax/eax-spec.pdf, and described in [EAX MO 2004]
EAX MO 2004	The EAX Mode of Operation, A Two-Pass Authenticated-Encryption Scheme Optimized for Simplicity and Efficiency, M. BELLARE, P. ROGAWAY, and D. WAGNER, January 18 2004, available from http://www.cs.ucdavis.edu/~rogaway/papers/eax.pdf
FIPS Pub 197	Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/N.I.S.T, Springfield, Virginia, November 26, 2001. Available from http://csrc.nist.gov/
NIST SP800-38A	Recommendation for Block Cipher Modes of Operation; Methods and Techniques. NIST Special Publication 800-38A 2001 Edition. US Department of Commerce/N.I.S.T, Springfield, Virginia, December 2001. Available from http://csrc.nist.gov/publications/nistpubs/800-38A/sp800-38A.pdf
NIST SP 800-38B	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. NIST Special Publication 800-38B 2001 Edition. US Department of Commerce/N.I.S.T, Springfield, Virginia, May 2005. Available from http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf
ISO/IEC 8824-1:2002	Information Technology—Abstract Syntax Notation One (ASN.1): Specification of Basic Notation
ISO/IEC 8824-2:2002	Information Technology—Abstract Syntax Notation One (ASN.1): Information Object Specification

ISO/IEC 8824-3:2002	Information Technology—Abstract Syntax Notation One (ASN.1): Constraint Specification
ISO/IEC 8824-4:2002	Information Technology—Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 Specifications
ISO/IEC 8825-1:2002	Information Technology—ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
ISO/IEC 8650-1:1996	Information Technology—Open Systems Interconnection—Connection-Oriented Protocol for the Association Control Service Element: Protocol Specification
ISO/IEC 15954:1999	Information Technology—Open Systems Interconnection—Connection-mode Protocol for the Application Service Object Association Control Service Element
ISO/IEC 15955:1999	Information Technology—Open Systems Interconnection—Connectionless Protocol for the Application Service Object Association Control Service
ISO/IEC 10035-1:1995	Information Technology—Open Systems Interconnection—Connectionless Protocol for the Association Control Service Element: Protocol Specification
ISO/IEC 646: 1991	ASCII character set
ATIS T1.667-1999	ATIS T1.667-2002 Intelligent Network (Revision of T1.667-1999): May 2002
NIST 800-38A - 2001	Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, 2001

2.3.6.2 ANSI C12.22 – Informative

FOLDOC: 2006	Free Online Dictionary of Computing; http://foldoc.org/ (retrieved on 2 May 2006)
HCCS 1: 1987	Handbook of Computer-communications Standards; Vol. 1: The Open Systems Interconnection (OSI) Model and OSI-related Standards, W. Stallings, Macmillan Publishing Co., Inc, 1987. ISBN: 0-02-948071-X
HCCS 2: 1987	Handbook of Computer Communications Standards, Vol. 2: Local Network Standards, W. Stallings, Macmillan Publishing Co., Inc, 1987. ISBN: 0-02- 948070-1
HCCS 3: 1988	Handbook of Computer-communications Standards. Vol. 3: Department of Defense (DoD) Protocol Standards, W. Stallings, Macmillan Publishing Co., Inc, 1988. ISBN: 0-02-948072-8
DND : 1993	Data Network Design: Packet-Switching Frame Relay 802.6\DQDB SMDS, ATM B-ISDN, SONET, Darren L. Spohn, McGraw-Hill Companies, 1993. ISBN: 0-07-060360-X
IPPA : 1995	Internetworking with TCP/IP Vol.1: Principles, Protocols, and Architecture, C. Douglas, Prentice Hall, 1995 (3rd edition) ISBN: 0-13-216987-8, 2000 (4th Edition), ISBN: 0-13-018380-6
OGUSPTO: 1976	Official Gazette of the United States Patent and Trademark Office (9434 O.G. 452 and 949 O.G. 1717), Aug 31, 1976
TCPCE : 1997	TCP/IP Clearly Explained, Pete Loshin, Academic Press Limited, 1997 (2nd Edition), ISBN: 0-12-455835-6